Virus Mydoom (suite): la variante 'B' vise Microsoft, une 3e version attendue

Après 4 jours de propagation, Mydoom (« ma destinée… ») se confirme bien comme le ver/virus e-mail le plus virulent qui ait jamais existé.

Les experts en sécurité informatique ont averti que les vers allaient perturber les messageries électroniques encore pour un certain temps, au moins jusqu'aux attaques programmées des sites internet des éditeurs de logiciels SCO et Microsoft prévues respectivement dimanche et mardi prochains. Selon Network Associates, le nombre d'ordinateurs infectés est passé de 100.000 à 200.000 mercredi à une fourchette comprise jeudi entre 400.000 et 500.000. La nouvelle variante (Mydoom-B) annoncée hier dans les forums de sécurité professionnels, est confirmée, telle que Trend Micro l'a l'identifiée. Il s'agit bien, là encore, d'un ver de type « mass-mailing » qui se diffuse au travers du carnet d'adresses en usurpant de vrais utilisateurs. Le ver continue de se propaser via le 'peer-to-peer' de Kasaa et dispose toujours d'une porte arrière (« back-door ») sur le port TCP 3127. Cette deuxième variante s'avère effectivement plus nuisible: elle interdit à l'hôte infecté de se mettre à jour auprès des différents éditeurs d'antivirus en écrasant le fichier HOSTS local et en rendant impossible les connexions vers une longue liste de sites (lire ci-après) où figurent les plus usités: ca.com, download.mcafee.com, f-secure.com, sophos.com, go.microsoft.com, networkassociates.com, symantec.com, kaspersky.ru, trendmicro.com… Mais sa propagation s'est en revanche avérée moins efficace que prévu. **Une troisième version redoutée** Mydoom-B était susceptible d'infecter les ordinateurs à la simple lecture du courriel la contenant, contrairement à son prédécesseur Mydoom.A: ce dernier ne s'active qu'à l'ouverture d'un fichier joint. Mais des défauts de fabrication ont heureusement bloqué cette fonction. Par contre les experts craigent l'apparition d'une troisième version, corrigée de ces anomalies. Comme son grand frère, la version B de Mydoom ouvre également une « back door » sur l'ordinateur infecté et permet à une personne extérieure de prendre le contrôle de la machine. Mydoom-B a fortement ralenti le réseau internet et la correspondance électronique en infectant plus de 100 millions de mails dans le monde au cours des 36 premières heures après son apparition, et près du tiers de la correspondance électronique après deux jours d'activité. Enfin, cette nouvelle version du ver est programmée pour s'attaquer à Microsoft, dont le site fera lui aussi l'objet d'une attaque par déni de service à partir du 1er février, tout comme celui de SCO. Comme SCO, la firme de Redmond a offert jeudi 250.000 dollars de récompense pour identifier la personne à l'origine du virus. L'éditeur avait également mis à prix la tête des créateurs de Blaster et SoBig. Sans succès. Avec **Norman Girard**, vulnerabilite.com (c) **Les sites d'anti-virus rendus non accessibles**

ad.doubleclick.net ad.fastclick.net ads.fastclick.net ar.atwola.com atdmt.com avp.ch avp.com avp.ru awaps.net banner.fastclick.net banners.fastclick.net ca.com click.atdmt.com clicks.atdmt.com dispatch.mcafee.com download.mcafee.com download.microsoft.com downloads.microsoft.com engine.awaps.net fastclick.net f-secure.com ftp.f-secure.com ftp.sophos.com go.microsoft.com liveupdate.symantec.com mast.mcafee.com mcafee.com media.fastclick.net msdn.microsoft.com my-etrust.com nai.com networkassociates.com office.microsoft.com phx.corporate-ir.net secure.nai.com securityresponse.symantec.com service1.symantec.com sophos.com spd.atdmt.com support.microsoft.com symantec.com update.symantec.com

updates.symantec.com us.mcafee.com vil.nai.com viruslist.ru windowsupdate.microsoft.com www.avp.ch www.avp.com www.avp.ru www.awaps.net www.ca.com www.fastclick.net www.f-secure.com www.kaspersky.ru www.mcafee.com www.microsoft.com www.my-etrust.com www.nai.com www.networkassociates.com www.sophos.com www.symantec.com www.trendmicro.com www.viruslist.ru www3.ca.com Cf: le site

Trend Micro